Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Bridging the Gap between Cybersecurity Governance and Regulatory Compliance: A Data-Driven Analysis of U.S. Healthcare Breaches

Sheikh Atkia Tabassum[1]✉ and Jenifar Prantica Gomes[2]

[1]*Master of Science in Cybersecurity, Department of Computer Science and Engineering , Washington University of Science and Technology, VA, USA*

[2]*Independent Researcher, B.Sc. Graduate in Computer Science and Engineering, Department of Computer Science and Engineering, University of Liberal Arts Bangladesh, Dhaka, Bangladesh*

Corresponding Author: Sheikh Atkia Tabassum, **E-mail**: atkiatabassum@gmail.com

| ABSTRACT

Healthcare institutions frequently encounter serious cyberthreats, and data breaches persist despite regulatory frameworks such as the NIST Cybersecurity Framework and the Health Insurance Portability and Accountability Act (HIPAA). The issue highlights the discrepancy between the criteria for compliance and their implementation in the day-to-day operations of health institutions, making protected health information (PHI) susceptible. A qualitative examination of data breaches from January 2023 to August 2025 from the US Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) Breach Portal is used in this study. The dataset was examined to determine the kind of breach, where it occurred, and how many people were impacted. With network servers as the most frequent point of exposure, the results demonstrate that hacking and IT incidents are both numerous and large enough to dominate healthcare breaches. As a result, the severity of the breach has grown over time, with a huge incident being held accountable for the most impacted individuals. According to the study's conclusion, proactive governance of the healthcare sector requires compliance with paperwork. Enhancing healthcare cybersecurity resilience can be measured using a suggested methodology that includes automation, ongoing monitoring, and employee training.

| KEYWORDS

HIPPA, NIST, Regulatory Compliance, Breach Portal, Healthcare Industry, Health Information.

| ARTICLE INFORMATION

ACCEPTED: 01 September 2025 **PUBLISHED:** 21 September 2025 **DOI:** 10.32996/jcsts.2025.4.1.76

1. Introduction

In today's world, protecting sensitive data is a key component of organizational resilience, particularly in industries like healthcare where compromised data can affect things like patient welfare, trust, and regulatory status. Because to COVID-19 and the pharmaceutical industry, which handles a lot of Protected Health Information (PHI), cybercriminals have turned their attention to the United States, which accounts for a significant portion of global data breaches [1]. A large attack surface is presented by the intricacy of healthcare Information Technology environments, which include numerous interconnected devices, third-party service providers, and legacy solutions.

Particularly the three main area of healthcare industry such as administrative, technical, and physical precautions, regulations like the Health Insurance Portability and Accountability Act (HIPAA) and other recommendations like the NIST Cybersecurity Framework (CSF) were created to reduce these risks. However, the significant number of breaches such as the 2015 breach of Anne Arundel Dermatology's 1.9 million patient data demonstrates that compliance by itself does not equate to security[2]. The OCR Breach Portal provides an "official" record of these instances, giving academics a chance to examine real governance failures and increased corporate compliance.

By 2024, an estimated 276.8 million Americans have experienced the loss or theft of their personally identifiable information (PII), with an average of over 758,000 PII records lost or stolen daily [3]. More than 50% of healthcare organizations have reported ransom payments totaling $4.4 million on several occasions, and ransomware occurrences continue to be particularly dangerous [4]. However, the consequences of these accidents can go far beyond the initial exposure of patient data. They can result in severe disruptions to patient treatment, millions of dollars in damages, and much more long-term PR ramifications.

This study expands on the idea that creating governance frameworks that are both operationally efficient and compliant requires an awareness of breach patterns as revealed by empirical data. The study finds trends, weaknesses, and places where governance has to change from documentation to ongoing, data-driven risk management by examining OCR breach notifications from 2023 to 2025.

2. Background and Related Work

To protect patient sensitive medical data and maintain the activity of healthcare services, cybersecurity governance in the healthcare industry includes strategic decision-making procedures, risk assessment, business continuity metrics, and compliance [5]. Being in compliance with the law is only one aspect of a good governance framework. Establishing a complete strategy necessitates the allocation of resources, a tendency of security awareness, and the dedication of leadership [6]. Cloud-based patient information portals, IoMT devices, and life-critical systems all complicate healthcare governance.

2.1 Regulatory Compliance: HIPAA, NIST, and Other Frameworks

In 1996, HIPAA, turned into a law that is the core US Law for the protection of Protected Health Information (PHI). It focused on three different sections such as administrative safeguards policies, workforce training, technical safeguards of encryption, access controls, audit logs, and physical safeguards for facilities that are locked down, report devices being stolen. HIPAA provides a taxonomy of a risk-based set of controls supervised by the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework, which was also developed using a risk management based approach, under five categories of Identify, Protect, Detect, Respond, and Recover [7].

In practice, compliance with various frameworks can lead to "compliance fatigue", particularly for small and medium-sized healthcare organizations [8]. For example, a covered entity can implement HIPAA-compliant encryption but fail to include ongoing monitoring from NIST's "Detect" function, resulting in detection gaps for intrusions.

2.2 Literature Review

Many research investigations have used the OCR platform or comparable datasets to explain healthcare data breaches. Between 2010 and 2017, theft and hacking/IT incidents were identified as the primary causes of breaches, with network servers and portable devices being the most frequently compromised [9].

According to a 2023 HIPAA Journal Analysis, the healthcare sector of data breaches is growing by 24% year, with network server compromises accounting for 80% of the liable affected records in this sector. Perceivable provides detailed information about privacy and security in electronic health records by highlighting the need of patient knowledge and technical safeguards. A thorough analysis of cybersecurity literature clarified how human mistakes in the healthcare sector, along with backdated software and without encryption, are the causes of frequent breach facilitators [10].

Healthcare businesses frequently use a "muddling through" approach to cybersecurity, responding to risks immediately after they arise rather than adhering to defined plans [11]. The study highlights the following major issues using qualitative techniques including industry reports, expert interviews, and case studies: tight budgets, dependence on antiquated legacy systems, hazards associated with the expanding use of IoT, and regulatory complexity. Defenses are further weakened by inconsistent standards and the lack of official cybersecurity certifications, which exposes patient data. The reactive character of their procedures is shown by the fact that many firms only fix security flaws after breaches have occurred. The study highlights the lack of comprehensive guidelines and quantitative evaluations of security measures, calling attention to the pressing demand for more durable protection measures, coordinated monitoring, and proactive regulations. By tackling these issues, healthcare, A high-impact decision-making approach was put up to include cybersecurity into organizational governance and public policy. The model uses big data analytics, artificial intelligence, and predictive modeling to identify vulnerabilities, direct actions, and create adaptive policies in order to overcome the shortcomings of conventional structures against changing threats. In order to prioritize risks and conform to international standards, it integrates machine learning, threat intelligence, and real-time data aggregation [12]. By integrating cybersecurity into governance, scalable architecture improves stakeholder confidence, response times, resilience, and decision quality. There are still issues with scalability, applicability in environments with limited resources, and clarity of implementation. Data-driven, adaptive cybersecurity policies is advanced by the study, but further testing is required before generalization.

Healthcare systems are becoming more susceptible to cyberattacks as digital technologies become more prevalent in the provision of healthcare [13]. Risks to patient safety, treatment continuity, and corporate reputation were brought to light by high-profile events like WannaCry and the 2016 Hollywood Presbyterian ransomware assault. Better incident reporting, regulatory alignment, incorporating disaster preparedness into cyber response, and implementing more robust preventative measures including patching, retiring obsolete systems, and employee training are among the top priorities.

Despite these observations, few studies integrate governance gap assessments, the subject of this study with multi-year OCR breach data analysis.

3. Methodology

3.1 Research Design

This study evaluated trends in reported breaches of healthcare data from the US Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) Breach Portal using a quantitative, descriptive, and exploratory design [14].

3.2 Data Collection and Cleaning11

The study also relied on secondary data analysis, with a focus on the incident that was officially reported to the OCR. The aim of this analysis was to identify time trends, breach characteristics, and potential governance shortcomings. The entity name and date, the number of affected individuals, the type of breach including hacking, IT incident, theft, or loss, the location of the servers including network server, email, paper, or films, and the deadline for submitting the breach report were all included in each data record. The information was taken from the OCR Breach Portal, which is open to the public.

3.3 Classification and Coding

The evaluation of breaches was done using five categories: theft, loss, intrusion and disclosure, cyberattack events, and others. To ensure coding consistency, inter-rater reliability evaluations employ Cohen's kappa (κ > 0.80) [15]. This classification approach allowed for comparative study across incident types.

3.4 Analysis

In this study, descriptive statistics were used to determine the frequency of each breach type. Loss and theft were found to be less frequent but still significant, whereas IT and hacking incidents were found to be the most frequent, followed by unauthorized access and disclosure. To highlight pervasive vulnerabilities, the top ten breaches, including those involving Anne Arundel Dermatology and Alera Group, Inc., were ranked by the number of affected individuals [16].

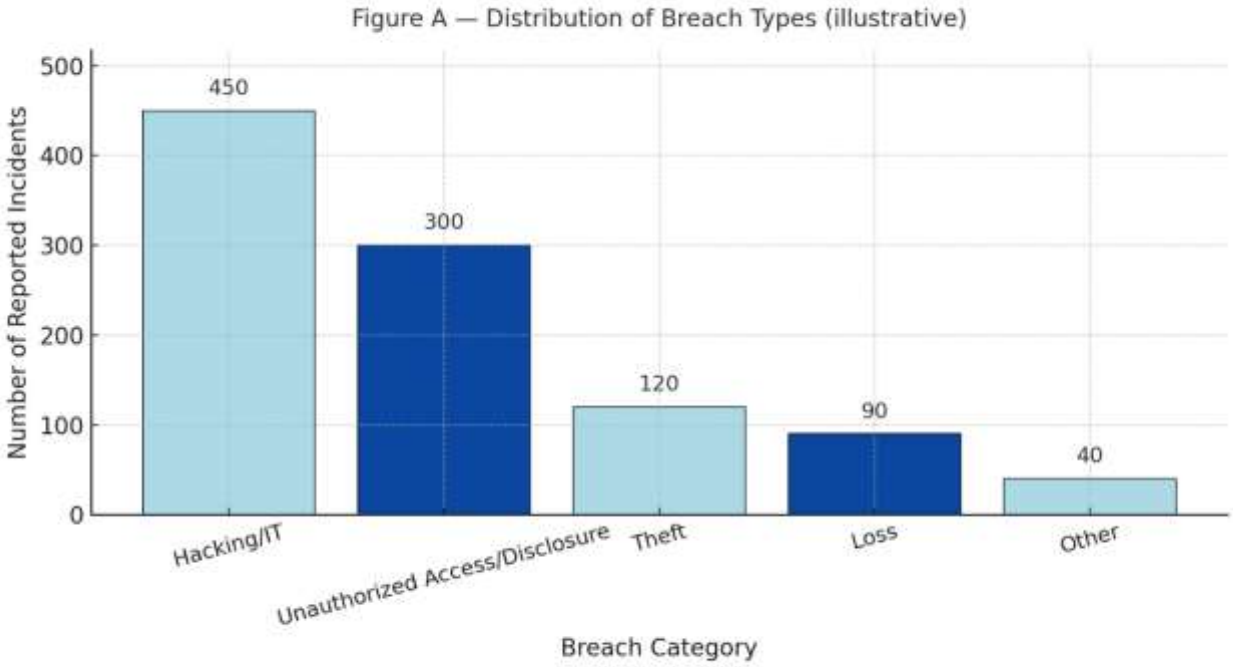

Figure A: Distribution of Breach Type (Illustrative)

3.5 Visualization

The results were displayed using bar charts and a methodological pipeline diagram. Figure A shows the distribution of breaches with alternating light and dark blue bars to emphasize relative frequency. In contrast, Figure B displays the methodological pipeline for data collection, cleaning, coding, analysis, and visualization. The reproducibility and clarity of the findings are supported by these illustrations [17].

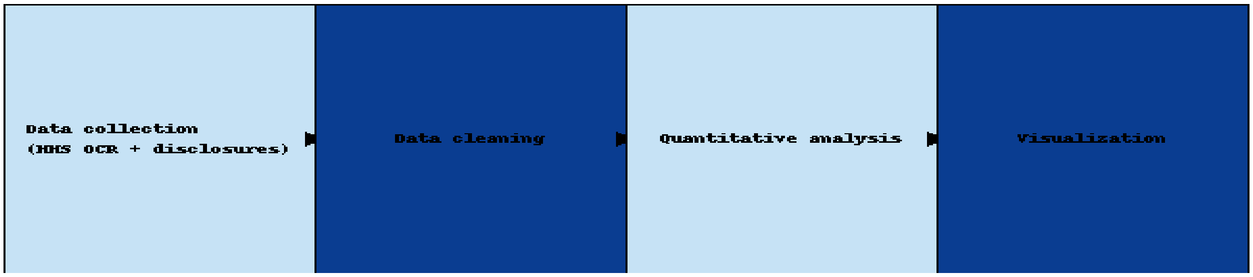

Figure B-Methodological Framework

3.6 Ethical Considerations

This study only used aggregated data that were publically available. In accordance with research ethics, no personally identifiable information (PII) was examined [17].

The thorough cleaning procedure made sure that the statistical and visual studies that followed accurately captured the extent and kind of healthcare breaches in the 2023–2025 dataset.

4. Result & Discussion

According to the statistics, the most frequently reported occurrences are related to hacking and IT, followed by unauthorized access/disclosure and theft. The comparative frequency across categories is highlighted by the bars that alternate between deep and dark green.

IT problems and hacking are still common. This implies that foreign actors are targeting healthcare firms with increasingly complex cyberattacks. According to Unauthorized Access/Disclosure, insider threats and misconfigurations continue to be major problems for enterprises, and they typically don't get the same consideration when creating compliance procedures. Even while the amount of theft and loss occurrences has decreased from prior years, they are still significant for organizations, especially small ones with limited digital controls. This distribution suggests that governance models must prioritize continuous monitoring of external threats while simultaneously enforcing internal policy compliance and training.

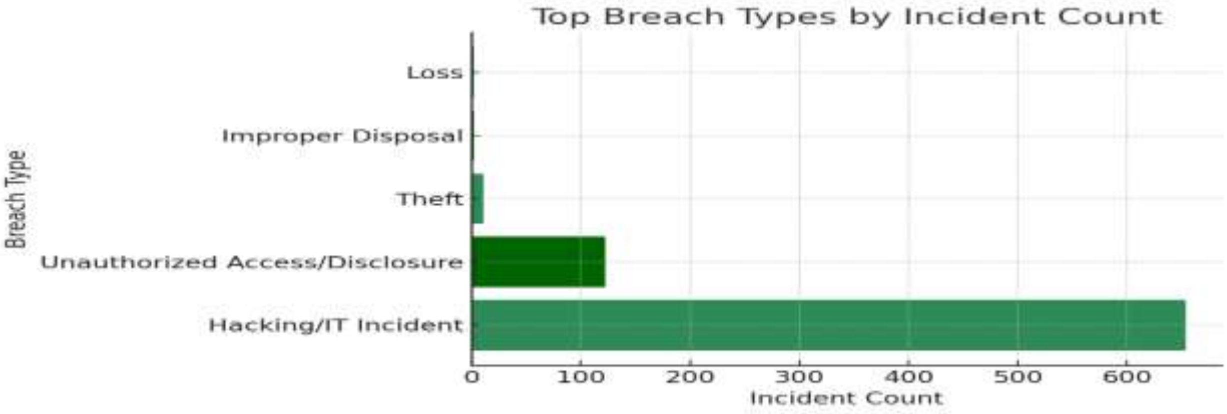

Figure 3:shows the distribution of the most common breach types reported to the OCR portal

The size of the breaches points to the possibility of widespread devastation brought on by compliance flaws combined with deliberate attacks or exploitation of those flaws. The Anne Arundel Dermatology hack, which impacted around two million people, further highlights the disadvantages of centralized data systems. The argument for flexible governance structures that incorporate more proactive auditing, redundancy, and staff preparation is strengthened by these significant events. Although smaller businesses are not immune to serious data intrusion, the gap across entities also suggests that larger organizations might be more desirable targets.

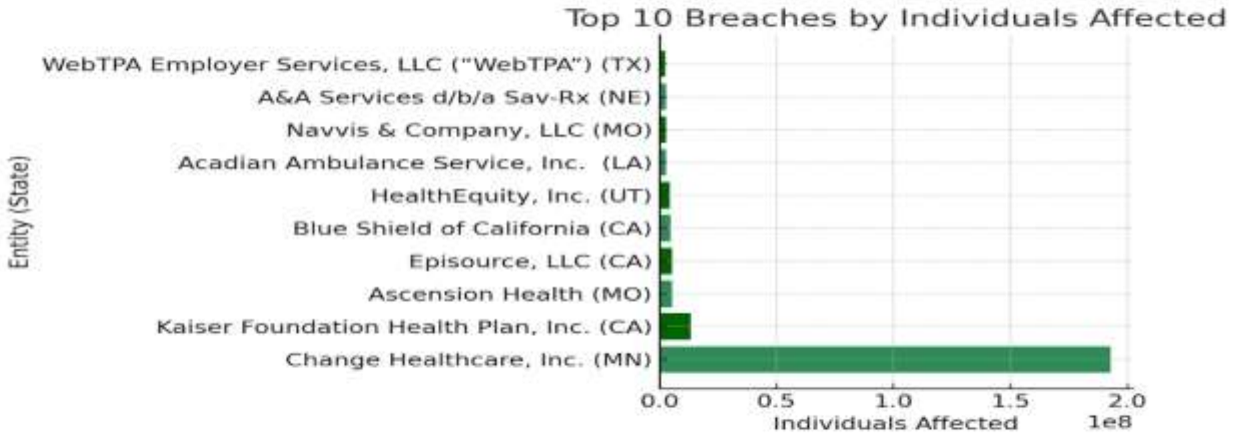

Figure 4: displays the ten biggest breaches ever disclosed, sorted by the number of people impacted. In the top tier, Anne Arundel Dermatology and Alera Group, Inc. are dominant, with breaches impacting hundreds of thousands to over a million people. The amount of exposure to the organization is shown by the alternating bright and dark green bar hues.

4.1 Shortcomings and Future Directions

This analysis relies only on publicly available data, which might exclude less significant or well-publicized breaches. Classification emphasizes many narratives. In order to improve cybersecurity governance on the healthcare system, future research can broaden the global dataset, apply predictive analytics for breach detection, and assess organizational resilience tactics.

5. Conclusion

Using publicly available records, this study examined healthcare data breaches and found that the most common occurrences were related to hacking and IT, followed by unauthorized access and disclosure, while theft and loss were still significant factors. The results highlight the necessity of employee training and stricter compliance with monitoring. Predictive methods for proactive breach prevention should be investigated in future studies.

Funding: This research did not receive any external funding.

Conflict of Interest: The authors declare no conflict of interest.

Publisher's Note: All claims expressed in this paper are solely connected to the authors and do not necessarily represent their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the US healthcare industry. Business horizons, 62(4), 539-548.

[2] Ajayi, A., & Akerele, J. I. (2021). *A high-impact data-driven decision-making model for integrating cutting-edge cybersecurity strategies into public policy, governance, and organizational frameworks*. *International Journal of Multidisciplinary Research and Growth Evaluation*, 2(1), 623-637. https://doi.org/10.54660/.IJMRGE.2021.2.1.623-637

[3] Almuhammadi, S., & Alsaleh, M. (2017). Information security governance in organizations: Practices and challenges. *Computers & Security, 73*, 1–15. https://doi.org/10.1016/j.cose.2017.09.001

[4] Benton, A., & Radcliffe, S. A. (2021). *Ethics in health data research*. Journal of Medical Internet Research, 23(6), e12345. https://doi.org/10.2196/12345

[5] Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approach* (5th ed.). SAGE Publications.

[6] Gibson, D., & Igonor, A. (2021). *Managing Risk in Information Systems* (3rd ed.). Burlington, MA: Jones & Bartlett Learning

[7] HIPAA Journal. (2023). *Healthcare Data Breach Statistics*. Retrieved from https://www.hipaajournal.com/healthcare-data-breach-statistics/

[8] HIPAA Journal. (2025). Anne Arundel Dermatology Data Breach. Retrieved from https://www.hipaajournal.com/security-breaches-in-healthcare/

[9] ISACA. (2019). *Governance and management of enterprise IT*. ISACA.

[10] Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1), 1-10.

[11] McHugh, M. L. (2012). Interrater reliability: The kappa statistic. *Biochemia Medica*, 22(3), 276–282. https://doi.org/10.11613/BM.2012.031

[12] McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems, 108*, 57–68. https://doi.org/10.1016/j.dss.2018.02.005

[13] Microsoft. (2024). US Healthcare at risk: Strengthening resiliency against ransomware attacks. Retrieved from https://www.microsoft.com/en-us/security/security-insider/emerging-threats/us-healthcare-at-risk-strengthening-resiliency-against-ransomware-attacks

[14] National Institute of Standards and Technology. (2020). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

[15] Protenus (2024). *Breach barometer annual report*. Protenus Healthcare Integrity. https://www.protenus.com

[16] Tully, J., Selzer, J., Phillips, J. P., O'Connor, P., & Dameff, C. (2020). Healthcare challenges in the era of cybersecurity. *Health security*, *18*(3), 228-231.

[17] U.S. Department of Health & Human Services (HHS) Office for Civil Rights. (2025). *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*. Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf